# REMARKS

**[0003]** Applicant respectfully requests reconsideration and allowance of all of the claims of the application. Claims 1-9, 12, 15-17, 19-31, 34-36, 38-39 and 41 are presently pending. Claims amended herein are 1, 15-17, 20, 34-36 and 39. Claims canceled herein are 10, 11, 13, 14, 32, 33 and 40. No new claims are added herein.

## Statement of Substance of Interview

**[0004]** The Examiner graciously talked with me—the undersigned representative for the Applicant—on Friday November 21, 2008. Applicant greatly appreciates the Examiner's willingness to talk. Such willingness is invaluable to both of us in our common goal of an expedited prosecution of this patent application.

**[0005]** During the interview, we discussed whether the proposed clarifying claim amendments differ from the cited reference, Scarfe. The Examiner was receptive to the proposals, and suggested combinations of features which would more fully distinguish the claims over the references of record. For example the Examiner was receptive to the combination of the features: "collecting message sequences" and applying "clustering" techniques as disclosed in the Application. However, the Examiner indicated that he would need to review the cited references more carefully and conduct another search, and requested that the proposed amendments be presented in writing.

**[0006]** The Applicant herein amends the claims in the manner discussed during the interview. Accordingly, Applicant submits that the pending claims are

allowable over the cited references for at least the reasons discussed during the interview.

**Formal Request for an Interview**

**[0007]** If the Examiner's reply to this communication is anything other than allowance of all pending claims, I formally request an interview with the Examiner. I encourage the Examiner to call me—the undersigned representative for the Applicant—so that we may resolve any outstanding issues quickly and efficiently over the phone. Accordingly, please contact me to schedule a date and time for a telephone interview that is most convenient for both of us. My contact information may be found on the last page of this response.

**Claim Amendments**

**[0008]** Without conceding the propriety of the rejections herein and in the interest of expediting prosecution, Applicant amends claims 1, 15-17, 20, 34-36 and 39 herein. Applicant amends claims to clarify claimed features. Such amendments are made to expedite prosecution and more quickly identify allowable subject matter. Such amendments are merely intended to clarify the claimed features, and should not be construed as further limiting the claimed invention in response to the cited references. Support for the claim amendments provided herein is found at least at pages 13-15 and page 27, lines 9-17 as set forth in the Application as originally filed. The claim amendments provided herein do not constitute new matter because they are supported by the Application as originally filed.

## Substantive Matters

**Claim Rejections under §§ 102 and 103**

**[0009]** Claims 1-17, 19-36 and 38-41 are rejected under 35 U.S.C. § 102 or § 103. In light of the amendments presented herein and the discussion during the above-referenced Examiner interview, Applicant submits that these rejections are moot. Accordingly, Applicant asks the Examiner to withdraw these rejections.

**[0010]** The Examiner rejects claims 1-4, 8-17, 19-23, 27-36 and 38-41 under § 102. For the reasons set forth below, the amended claims provided herein should not be considered anticipated by the reference of record.

**[0011]** In addition, the Examiner rejects claims 5-7 and 24-26 under § 103. For the reasons set forth below, these claims should not be considered obvious because in light of the claim amendments provided herein the references of record are not sufficient to render a prima facie case showing that the claims are obvious.

**[0012]** Accordingly, Applicant respectfully requests that the § 102 and § 103 rejections be withdrawn and the case be passed along to issuance.

**[0013]** The Examiner's rejections are based upon the following references alone or in combination:

- **Scarfe:** *Scarfe, et al.,* US Patent Publication No. 2004/0103021 (published May 27, 2004); and
- **Greifeneder:** *Greifeneder, et al.,* US Patent Publication No. 2004/0243349 (published December 2, 2004).

**Overview of the Application**

**[0001]** The Application describes a technology for investigating the behavior of an environment by analyzing messages passed between participants in the environment. The environment can pertain to a network, a machine, a system, a software program, or other environment. The analysis can use any kind of analysis to group sequences of messages into a collection of related sequences. The results of the analysis may reveal anomalous conditions within the environment, or other features of the environment. (Application, Abstract).

**Cited References**

**[0002]** The Examiner cites Scarfe as the primary reference in the anticipation and obviousness-based rejections. The Examiner cites Greifeneder as a secondary reference in the obviousness-based rejections.

*Scarfe*

**[0003]** Scarfe describes a technology for classifying network traffic events in accordance with one or more conditions comprising categorizing means for categorizing a plurality of network traffic events, analysing means for analysing at least one aspect of the network traffic events and identifying groups in accordance with the analysis, group determining means for determining group allocation for the categorized network traffic events, generating means for generating one or more conditions in relation to the group and category of analyzed network traffic events, and classifying means for classifying a newly

detected network traffic event in accordance with the one or more conditions generated. (Scarfe, Abstract).

*Greifeneder*

**[0004]** Greifeneder describes a technology for monitoring and analysis of networked systems, that is non-intrusive and real time. Both secure and non-secure traffic may be analyzed. The provided method involves non-intrusively copying data from a communication medium, reconstructing this data to a higher level of communication, such as the application level, grouping the data into sets, each set representing a session, and organizing the data for chosen sessions in hierarchical fashion which corresponds to the hierarchy of the communicated information. If monitored communications are encrypted, they are non-intrusively decrypted in real time. Hierarchically reconstructed session data is used by one or more plug-in applications, such as alarms, archival applications, visualization applications, script generation applications, abandonment monitoring applications, error detection applications, performance monitoring applications, and others. (Greifender, Abstract).

# Anticipation Rejections

**[0005]** Applicant submits that the anticipation rejections are not valid in light of the amended claims set forth herein because, for each claim, no single reference discloses each and every element of the claim.[1] Furthermore, the elements disclosed in the single reference are not arranged in the manner recited by each rejected claim.[2]

## Based upon Scarfe

**[0006]** The Examiner rejects claims 1-4, 8-17, 19-23, 27-36 and 38-41 under 35 U.S.C. § 102(e) as being anticipated by Scarfe. Applicant respectfully submits the amended claims set forth herein and traverses the rejection of these claims and requests the Examiner to withdraw the rejection of these claims.

*Independent Claim 1*

**[0007]** Applicant submits that Scarfe does not disclose at least the following elements and features as recited in this amended claim (in part, with emphasis added):

> **"converting identifying information** pertaining to the at least one participant **into an indication of a role played by the at least one participant** in the message-passing environment"

---

[1] "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987); also see MPEP §2131.

[2] See *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990).

"assembling the messages into at least one message sequence, wherein assembling includes **combining multiple message traces into the at least one message sequence**, each message trace pertaining to one or more messages transmitted by, or received at, a participant, **wherein the combining is based on one or more of, a specified participant, a specified time frame, a transaction nature and the role played by the at least one participant**"

"**wherein the analyzing comprises comparing at least one message sequence with a reference message sequence**, the reference message sequence comprises at least one of a sequence **that reflects an error-free operation in the message passing environment and a sequence that reflects known failure conditions in the message passing environment**"

"**performing cluster analysis** to group the at least one message sequence into at least one cluster, wherein the cluster analysis **includes forming a data matrix based on information in the at least one message sequence and forming the at least one cluster based on the data matrix**"

**[0008]** Clarifying amendments were added to independent claim 1 to further distinguish the claim over the cited references. Accordingly, the Applicant asserts that Scarfe does not disclose each and every feature and element of amended independent claim 1.

**[0009]** The Examiner cited Scarfe for its teachings of (Action, p. 2):

> collecting a plurality of messages –([0010] e.g., log) from at least one participant –([0030], e.g. IP addresses) in the message-passing environment -([FIG 1]) , wherein each message has a first piece describing transfer information – ([0010] e.g. source/destination IP address) and a second piece describing an operation being performed in the message – ([COL 8], [Table 1] e.g., No. packets sent by IP address, i.e., operation)

**[0010]** The teaching of Scarfe of "source/destination IP address" does not disclose "converting identifying information… into an indication of a role played by the at least one participant" as recited in amended independent claim 1.

**[0011]** The Examiner cited Scarfe for its teachings of (Action, pp. 2-3):

> assembling the messages into at least one message sequence- ([0030-31], [FIG 8], [0055] e.g., applicant's instant specification discusses a "message sequence" as any grouping of one or more messages. Here, Scarfe et al. teaches categorizing (e.g., grouping) network traffic into IP address. The messages are accumulated over specific time periods and categorized (e.g., grouped : classification of IP addresses using time periods) according to the IP address. It is interpreted that messages per IP source are grouped together for analysis and subsequently assigned a cluster, such as cluster G. For example, as in a case of an attack from an IP source over successive period within 24 hrs, it would be possible to assign this activity to a cluster)

**[0012]** Scarfe was cited for teaching "categorizing (e.g. grouping) network traffic in to IP address… classification of IP address using time periods", however this teaching of Scarfe is limited in its application and does not disclose the following elements and features of amended independent claim 1: "assembling the messages… combining multiple message traces into the at least one message

sequence... wherein the combining is based on one or more of, a specified participant, a specified time frame, a transaction nature and the role played by the at least one participant."

**[0013]** Additionally, the Examiner cited Scarfe for its teachings of the following (Action, p. 3):

> Paragraph [0031] discusses that changes in cluster classification between successive time periods provides information about the behavior of an IP address. In effect, it is interpreted that categorized messages are compared using cluster assignments), the reference message sequence comprises a sequence that reflects an error- free operation in the message passing environment ([COL 9 – element N] e.g., cluster assignment corresponding to categorized IP messages for that time period, where cluster N is identified as normal. 'Reference' is interpreted to mean that a comparison takes place between subsequent message groupings)

**[0014]** The Examiner asserted that Scarfe teaches "...cluster assignment corresponding to categorized IP messages for that time period, where cluster N is identified as normal... [and] 'Reference' is interpreted to mean that a comparison takes place between subsequent message groupings." However, "cluster N identified as normal" as found in Scarfe is **not** a "reference message sequence... that reflects an error-free operation in the message passing environment and a sequence that reflects known failure conditions in the message passing environment" as recited in amended independent claim 1. Further, the "categorized IP messages for that time period" as found in Scarfe is **not** "comparing at least one message sequence with a reference message sequence" as recited in amended independent claim 1.

**[0015]** Further, Scarfe does not disclose "performing cluster analysis to group the at least one message sequence into at least one cluster, wherein the cluster analysis includes forming a data matrix based on information in the at least one message sequence and forming the at least one cluster based on the data matrix" as recited in amended independent claim 1.

**[0016]** Consequently, Scarfe no longer supports a rejection of amended claim 1 on the basis of anticipation under §102 because Scarfe does not disclose each and every element and feature of the claim. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim for at least these reasons.

*Dependent Claims 2-4, 8-17, 19 and 40*

**[0017]** These claims ultimately depend upon amended independent claim 1. As discussed above, amended independent claim 1 is allowable. It is axiomatic that any dependent claim which depends from an allowable base claim is also allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

*Independent Claim 20*

**[0018]** Applicant submits that Scarfe does not disclose at least the following elements as recited in this amended claim (in part, with emphasis added):

**"cluster analysis logic** configured to perform cluster analysis to group the at least one message sequence into at least one cluster, wherein the cluster analysis logic is **configured to form a data matrix based on information in the at least one message sequence and form the at least one cluster based on the data matrix"**

**[0019]** The Applicant asserts that Scarfe does not disclose each and every element and feature of amended independent claim 20. Without needlessly repeating the discussion and evidence above in regard to amended independent claim 1, amended independent claim 20 is allowable for at least the same or similar reasons provided above in support of amended independent claim 1 because the clarifying amendments made to amended independent claim 1 are not disclosed by Scarfe. Therefore as explained and shown above in regards to amended independent claim 1, Scarfe does not disclose all of the elements and features of this claim. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim for at least these reasons.

*Dependent Claims 21-23, 27-36, 38 and 41*

**[0020]** These claims ultimately depend upon amended independent claim 20. As discussed above, amended independent claim 20 is allowable. It is axiomatic that any dependent claim which depends from an allowable base claim is also allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

*Independent Claim 39*

**[0021]** Applicant submits that Scarfe does not disclose at least the following elements as recited in this amended claim (in part, with emphasis added):

> "means for **converting identifying information** pertaining to the at least one participant **into an indication of a role played by the at least one participant** in the message-passing environment"
>
> "means for assembling the messages into at least one message sequence, wherein assembling includes **combining multiple message traces into the at least one message sequence**, each message trace pertaining to one or more messages transmitted by, or received at, a participant, **wherein the combining is based on one or more of, a specified participant, a specified time frame, a transaction nature and the role played by the at least one participant**"
>
> "wherein the **means for analyzing comprises comparing at least one message sequence with a reference message sequence**, the reference message sequence comprises at least one of a sequence **that reflects an error-free operation in the message passing environment and a sequence that reflects known failure conditions in the message passing environment**"
>
> "means for **performing cluster analysis** to group the at least one message sequence into at least one cluster, wherein the cluster analysis includes **forming a data matrix based on information in the at least one message sequence and forming the at least one cluster based on the data matrix**"
>
> "means for **storing the at least one message in a master collection of message sequences**"

"means for **culling the master collection of message sequences for at least one subset of a message sequence based on specified criteria including one of more of**: a specified time range, transaction type, participants involved in at least one message exchange, objectives of an analyst and a nature of the message-passing environment involved"

"means for **storing the at least one subset for subsequent analysis**"

**[0022]** Scarfe does not disclose each and every element and feature of amended independent claim 39. Without needlessly repeating the discussion and evidence above in regard to amended independent claim 1, amended independent claim 39 is allowable for at least the same or similar reasons provided above in support of amended independent claim 1 because the clarifying amendments made to amended independent claims 1 and 39 are not disclosed by Scarfe.

**[0023]** In addition, amended independent claim 39 includes further clarifying amendments which are not disclosed by Scarfe. Specifically, amended independent claim 39 recites "means for storing the at least one message in a master collection of message sequences" which is not disclosed by Scarfe. Amended independent claim 39 also recites "means for culling the master collection of message sequences for at least one subset of a message sequence based on specified criteria..." which is not disclosed by Scarfe. Further, amended independent claim 39 recites "means for storing the at least one subset for subsequent analysis" which is not disclosed by Scarfe.

**[0024]** Consequently, as explained and shown above in regards to amended independent claim 1 and as shown by the further clarifying amendments of amended independent claim 39, Scarfe does not disclose all of the elements and features of this claim 39. Thus, Scarfe does not anticipate this amended claim. Accordingly, the Applicant asks the Examiner to withdraw the rejection of amended independent claim 39.

## Obviousness Rejections

**Lack of *Prima Facie* Case of Obviousness (MPEP § 2142)**

**[0025]** Applicant disagrees with the Examiner's obviousness rejections. For the reasons set forth below, these claims should not be considered obvious, because, in light of the claim amendments provided herein, the references of record are not sufficient to support a prima facie case showing that the claims are obvious in view of Scarfe and Greifender.

**Based upon Scarfe and Greifeneder**

**[0026]** The Examiner rejects claims 5-7 and 24-26 under 35 U.S.C. § 103(a) as being unpatentable over Scarfe and Greifeneder. The Applicant respectfully submits claim amendments herein, traverses the rejection of these claims and asks the Examiner to withdraw the rejection of these claims.

*Dependent Claims 5-7*

**[0027]** These claims ultimately depend upon amended independent claim 1. As discussed above, amended independent claim 1 is allowable over Scarfe. It is axiomatic that any dependent claim which depends from an allowable base claim is also allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons over the combination of Scarfe and Greifeneder.

**[0028]** The Examiner cited Greifeneder to compensate for deficiencies of Scarfe. The Examiner cited Greifeneder for teaching (Action, p. 11):

> language. Greifeneder et al teaches that network traffic may comprise documents including XML, GIF, and JPG communicated using network protocols, including but not limited to SOAP ([0064], [0019])
>
> Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to modify Scarfe et al. to include xml based messages. Scarfe et al. teaches collecting information pertaining to network traffic for classification and analysis. Greifeneder et al. teaches a method and system for monitoring and the analysis of networked systems. Xml base messages are a common format utilized in network communication. Since xml messages include data about data, it would have been obvious to group and analyze such messages for pertinent information about the behavior of a sender/receiver within a network.
>
> 34. As per claims 6 and 25, Greifeneder et al. teaches wherein the markup language is xml ([0064] e.g. XML)
>
> 35. As per claims 7 and 26, Greifeneder et al. teaches wherein the network uses Simple Object Access Protocol to transmit messages between participants ([0019] e.g. SOAP)

**[0029]** However, without addressing whether Greifeneder teaches "documents including XML, GIF, and JPG communicated using network protocols, including but not limited to SOAP... a method and system for monitoring and the analysis of network communication," the Applicant asserts that Greifeneder does not teach or suggest the elements and features of amended independent claim 1 which were not taught or disclosed in Scarfe. Specifically, the Applicant asserts that Greifeneder does not teach or suggest the following as recited in amended independent claim 1 (in part and with emphasis added):

**"converting identifying information** pertaining to the at least one participant **into an indication of a role played by the at least one participant** in the message-passing environment"

"assembling the messages into at least one message sequence, wherein assembling includes **combining multiple message traces into the at least one message sequence**, each message trace pertaining to one or more messages transmitted by, or received at, a participant, **wherein the combining is based on one or more of, a specified participant, a specified time frame, a transaction nature and the role played by the at least one participant"**

"**wherein the analyzing comprises comparing at least one message sequence with a reference message sequence**, the reference message sequence comprises at least one of a sequence **that reflects an error-free operation in the message passing environment and a sequence that reflects known failure conditions in the message passing environment**"

"**performing cluster analysis** to group the at least one message sequence into at least one cluster, wherein the cluster analysis **includes forming a data matrix based on information in the at least one message sequence and forming the at least one cluster based on the data matrix**"

**[0030]** Thus, the combination of Scarfe and Greifeneder fails to teach or suggest each and every feature and element of amended independent claim 1. Therefore, because claims 5-7 depend from amended independent claim 1, claims 5-7 cannot be considered obvious in light of the combination of Scarfe and Greifeneder. Accordingly, the Applicant respectfully asks the Examiner to withdraw the rejection of these claims for at least these reasons.

*Dependent Claims 24-26*

**[0031]** These claims ultimately depend upon amended independent claim 20. As discussed above, amended independent claim 20 is allowable over Scarfe. It is axiomatic that any dependent claim which depends from an allowable base claim is also allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

**[0032]** The Examiner cited Greifeneder to compensate for the deficiencies of Scarfe. As explained above in regard to dependent claims 5-7, Greifeneder does not teach or suggest the elements and features of amended independent claim 1 which are not taught or suggested by Scarfe. Amended independent claim 20 includes amendments similar to those added to independent claim 1. Therefore because Greifeneder does not compensate for the deficiencies of Scarfe as to amended independent claim 1, the combination of Scarfe and Greifeneder is also insufficient to teach or suggest each and every feature of amended independent claim 20. Accordingly, because claims 24-26 depend from allowable amended independent claim 20, claims 24-26 should not be considered obvious in light of Scarfe and Greifeneder. Accordingly, the Applicant respectfully asks the Examiner to withdraw the rejection of these claims for at least these reasons.

**Dependent Claims**

**[0033]** If not addressed individually above, in addition to its own merits, each dependent claim is allowable for the same reasons that its base claim is allowable. Applicant requests that the Examiner withdraw the rejection of each dependent claim where its base claim is allowable.

## Conclusion

**[0034]** All pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the application. If any issues remain that prevent issuance of this application, the **Examiner is urged to contact me before issuing a subsequent Action**. Please call or email me at your convenience.

Respectfully Submitted,

Lee & Hayes, PLLC
Representatives for Applicant

/Jacob S. Scott/ Dated: 2008-11-26

Jacob S. Scott (Jake@leehayes.com)
Registration No. 62,806
John Meline (Johnm@leehayes.com; x4757)
Registration No. 58,280
Customer No. **22801**
Telephone: (509) 944-4728
Facsimile: (509) 323-8979
www.leehayes.com